CUSTOMIZABLE CRYPTOGRAPHIC DEVICE

Russell D. Housley Gregory W. Piper Randy V. Sabett

5 ABSTRACT

The invention enables a cryptographic device to be easily, securely and/or irreversibly customized to provide specified cryptographic functionality. For example, the invention can enable easy and secure modification (expansion, 10 reduction or changing) of application code (which interacts with code stored on a cryptographic device) via the exposure of, for example, the mathematical primitive operations available on the cryptographic device. In particular, the invention can enable modification of available cryptographic 15 operations at a relatively high level of programming abstraction, thus enabling such modification to be accomplished relatively easily. Further, the invention can enable the modification to be accomplished in a manner that does not necessitate or allow access by the application 20 developer to other operations of the cryptographic device, thus providing security for the proprietary code and/or cryptographic keys of other persons or entities that may be present on the cryptographic device. The invention can also enable specification of permissible cryptographic 25 characteristics of a cryptographic device from a set of

available cryptographic characteristics of the cryptographic In particular, such specification can be done (at device fulfillment, for example) in a manner that is irreversible, thus enabling the cryptographic device to 30 satisfy export regulations for cryptographic devices and/or

to meet customer requirements for device security.